Angelique "Q" Napoleon

CYBERSECURITY

NAHMA Cyber Awareness

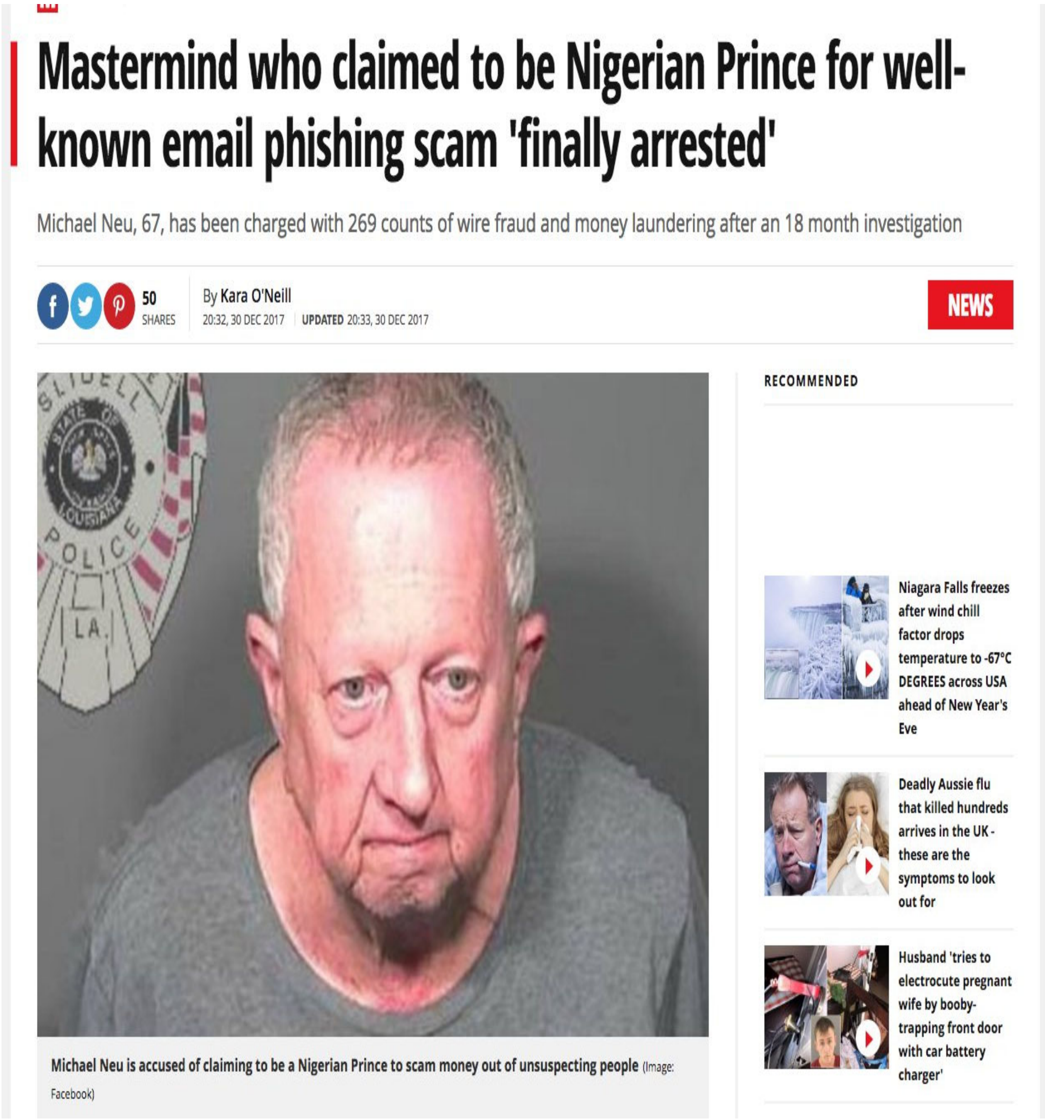
Why is Cybersecurity Important

- Persistent cyber threats continue to plague organizations of all sizes and across all industries.
- These organizations can be secure only with the active participation from EVERYONE.
- Effective security must be enterprise-wide, involving everyone in fulfilling security responsibilities.
- Each of you has a role in Cybersecurity from the newest employee to the chief executive officer.
- You have the power to harm or to help, to weaken or strengthen, the organization’s security posture

New Vehicle Purchases in 2024

Who doesn’t love getting a new automobile? If you decide to trade in your vehicle, consider doing the following **BEFORE** you go to the dealership:

- Do a **FACTORY RESET** of your Infotainment Center **TWICE** – this will erase ALL data that has been sync’d to the vehicle.
- Double Check the reset was successful by checking the Navigation System to make sure **YOUR** home location is blank.
- Make sure your iTunes or Spotify accounts are no longer sync’d to the vehicle.
- If you have On-Star contact them to **DIRECTLY** cancel the subscriptions and any additional phone lines you have for the vehicle.



Mastermind who claimed to be Nigerian Prince for well-known email phishing scam 'finally arrested'

Michael Neu, 67, has been charged with 269 counts of wire fraud and money laundering after an 18 month investigation

50 SHARES

By Kara O'Neill
20:32, 30 DEC 2017 | UPDATED 20:33, 30 DEC 2017

NEWS

Michael Neu is accused of claiming to be a Nigerian Prince to scam money out of unsuspecting people (Image: Facebook)

RECOMMENDED

Niagara Falls freezes after wind chill factor drops temperature to -67°C DEGREES across USA ahead of New Year's Eve

Deadly Aussie flu that killed hundreds arrives in the UK - these are the symptoms to look out for

Husband 'tries to electrocute pregnant wife by booby-trapping front door with car battery charger'

Cybercriminals Never Rest!

Cybercriminals never rest and it's important to protect your digital identity as well as you heart!!

With COVID we saw on-line dating surge across the world with so many locked in their homes for weeks at time it was a cyber criminals dream come true. They could essentially become anyone!

Cat-Phishing is a type of **ONLINE SCAM** where someone creates a fake online identity to lure unsuspecting victims into a relationship or a fraudulent scheme.

It can result in some damaging impcts for the victim, including financial losses and identity theft as well as mental trauma.

One of the most popular scams is the Nigerian Prince Scam!

Dating Sites

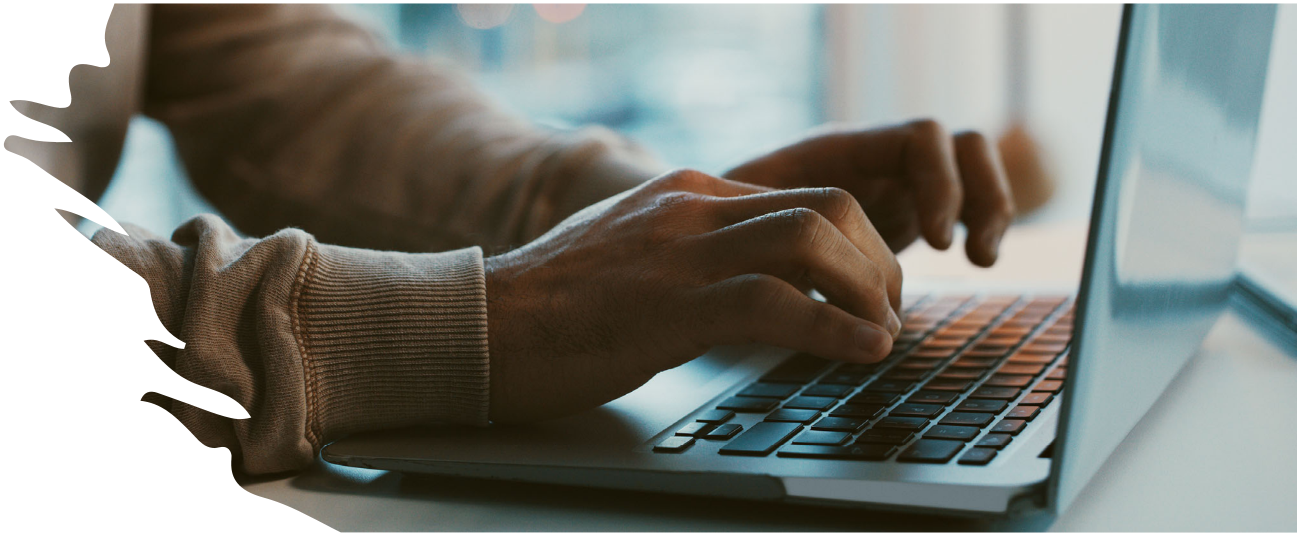
- There are many on-line dating sites that cater to specific demographics, interests, religions, professions and the list goes on and on.

- These sites offer an individual the opportunity to connect with people from around the world.

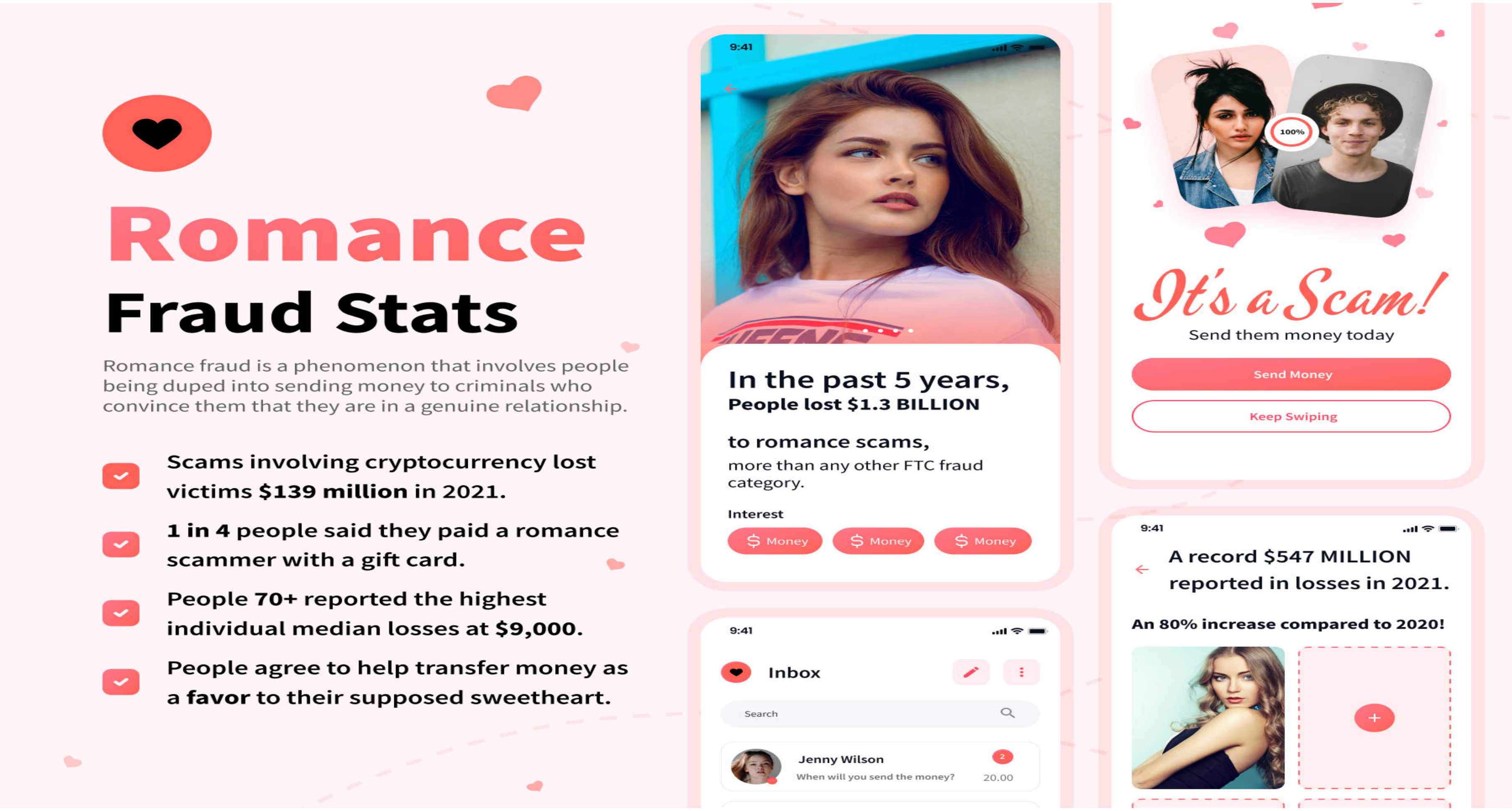
- Long Distance dating has never been easier with FaceTime, WebEx, Zoom and other video conferencing capabilities as well as social media.

- Be aware of scammers on these platforms

- Not all dating sites are full of scammers just be careful!



How Real Is It?



Romance Fraud Stats

Romance fraud is a phenomenon that involves people being duped into sending money to criminals who convince them that they are in a genuine relationship.

- ✓ Scams involving cryptocurrency lost victims **$139 million** in 2021.
- ✓ **1 in 4** people said they paid a romance scammer with a gift card.
- ✓ People 70+ reported the highest individual median losses at **$9,000.**
- ✓ People agree to help transfer money as a **favor** to their supposed sweetheart.

9:41

In the past 5 years,
People lost $1.3 BILLION

to romance scams,
more than any other FTC fraud category.

Interest

9:41

Jenny Wilson
When will you send the money?
2
20.00

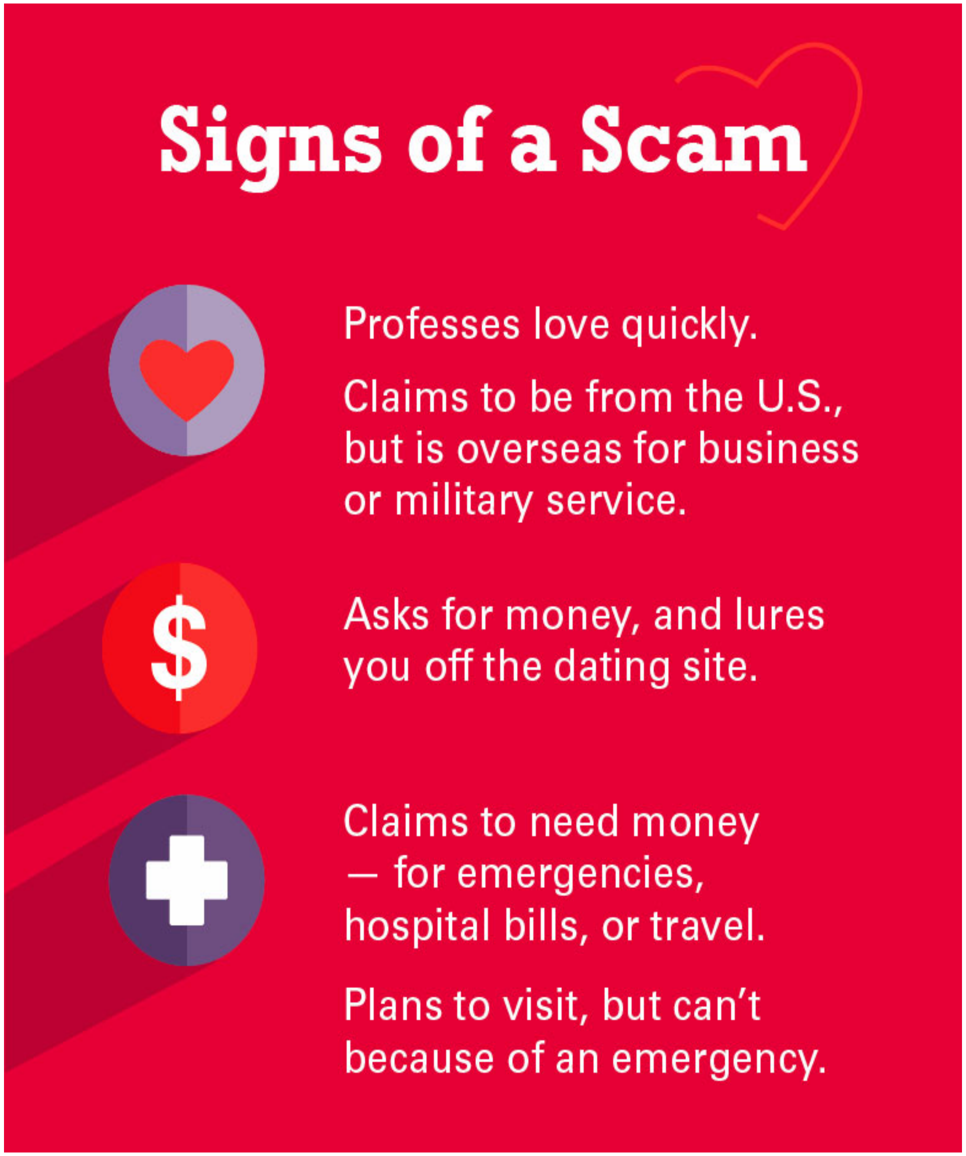
It's a Scam!

Send them money today

9:41

A record $547 MILLION reported in losses in 2021.

An 80% increase compared to 2020!



Signs of a Scam

Professes love quickly.

Claims to be from the U.S., but is overseas for business or military service.

Asks for money, and lures you off the dating site.

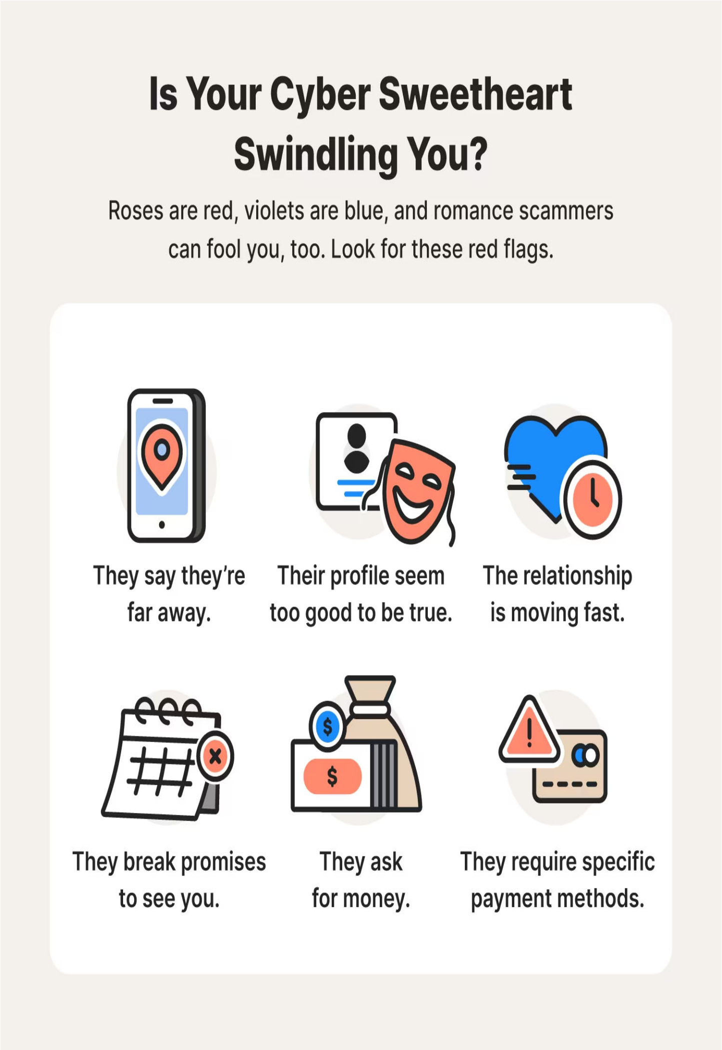
Claims to need money — for emergencies, hospital bills, or travel.

Plans to visit, but can't because of an emergency.

What To Look For

Signs of a scam are no different in real life!

- Be careful how much information you share with a stranger
- Never list your place of employment on a dating site
- Pay attention to those red flags!
- Don't access dating sites on work computers
- Don't send money through the dating sites or social media
- Don't click links they send you



Is Your Cyber Sweetheart Swindling You?

Roses are red, violets are blue, and romance scammers can fool you, too. Look for these red flags.

They say they're far away.

Their profile seem too good to be true.

The relationship is moving fast.

They break promises to see you.

They ask for money.

They require specific payment methods.

Check Your Profile(s)

Sometimes we invite problems into our lives that could have been avoided!

Check your social media and dating site profiles to make sure you aren't giving away too much information and making yourself a target!

Recommended Removals or Changes:

- Any reference to being a widow
- Specifics about your profession
- Specifics about where you live (full address)
- Using Pictures with specifics (remove the meta data it has exact location)
- Pictures with your family (kids, ect)
- Linking a credit card with the account
- Never give your work information

Money / Money Management

Avoiding Scams and Fraud for Older Adults

Older adults lose billions of dollars each year to scams and fraud. Get tips to protect yourself and your money. Learn how to spot common scams, keep your money secure, and

financial fraud if you suspect you're a victim.

The Victims Are Real

The profile might be fake but the victims are very real!

This isn’t just happening to older American’s, it’s even happening to the younger generations.

Pay attention to the red flags and know the signs of a love scam!

Its very easy to become “attached” or fall in love with someone when they say all the right things. We are human and its important to protect yourself, your identify and your information!

The financial losses have been staggering and they rarely get recovered!

Artificial Intelligence

Thanks to AI it's easier than ever to spoof or fake out an online discussion, video chat or even a call!

Do you know who you're really talking to?

Pay attention to the callers images, if they freeze or "skip" it's AI generated

Avoid the tricks by being aware of the tactics

DO NOT respond to unsolicited emails or telephone calls from an unknown or untrusted source.

VERIFY the identity of an individual claiming to represent an organization by contacting the organization directly. Caller ID can be spoofed so call known numbers back if you think it's a scam

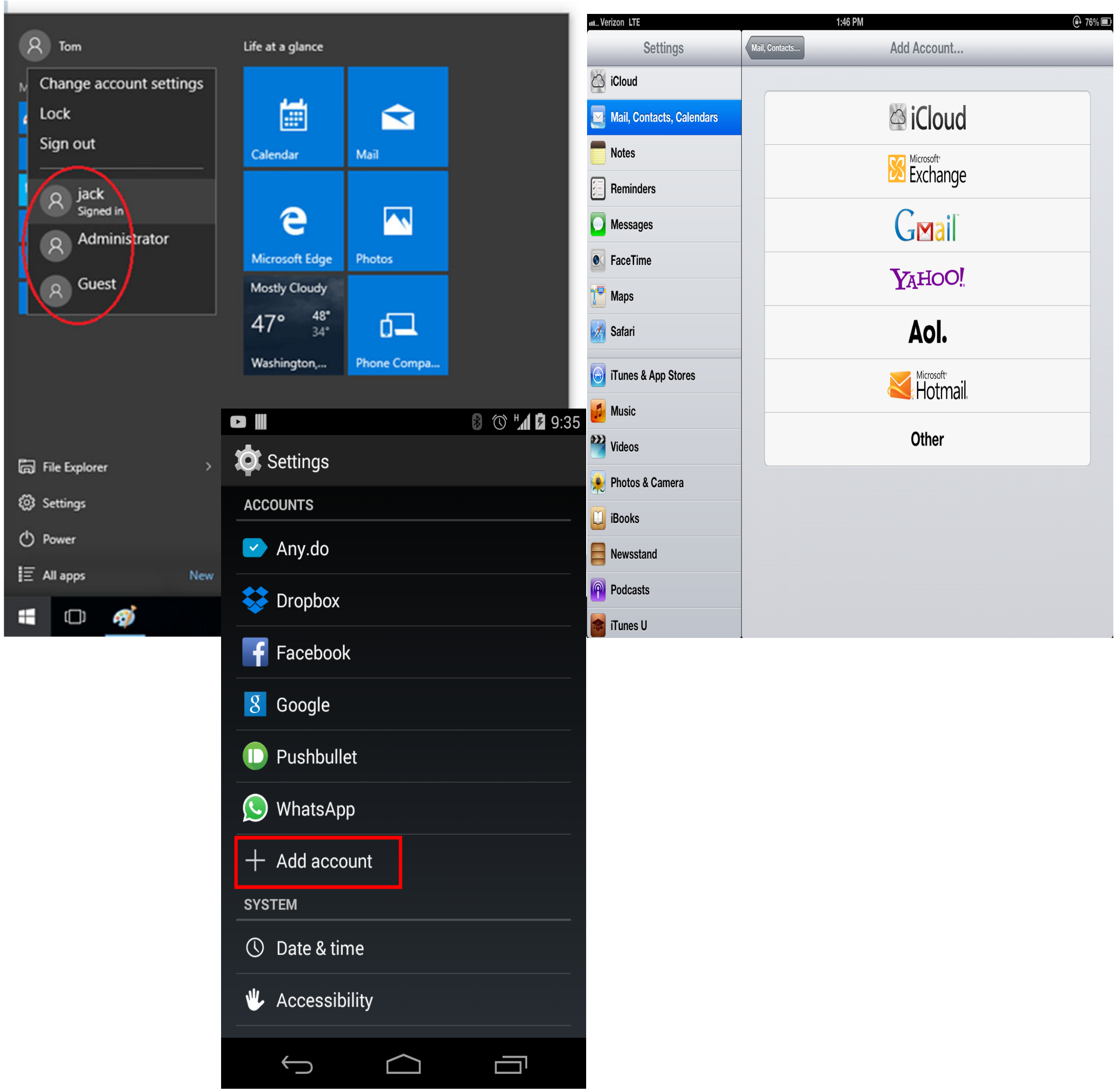
BE AWARE of emails that ask you to verify your information or provide sensitive information. Do not open attachments contained in a suspicious email.

UPDATE MALWARE SCANNERS on your devices.

AUTOMATICALLY UPDATE your security software, operating system, and web browser. DO NOT WAIT!

BE AWARE of the applications you load on your phone and devices – they access more information that you are aware of!

DISCUSS security awareness best practices with your family, friends, colleagues.

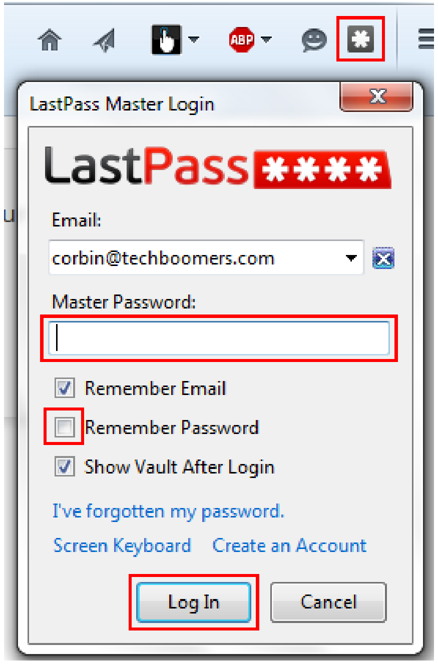


User Account Maintenance

User Accounts on your devices require frequent maintenance. It's important to review the following:

- Password Strength (12-14 characters/numbers/symbols/special characters)
- Password Age (is it older than 12 months?)
- Do you still use the app? If not **DELETE IT!**
- Are you using default passwords? Change them!
- Consider enabling Multi-Factor Authentication for your apps that it can used on
- Social Media – change passwords and review for fake accounts
- Social Media – review settings and make sure your profile is **PRIVATE**
- Social Media – consider creating a rescue account

Password Managers



Email: corbin@techboomers.com

Master Password:

☑ Remember Email

□ Remember Password

☑ Show Vault After Login

KeePass

dashlane vs. LastPass

or...

1Password

KeePass Password Safe

RoboForm

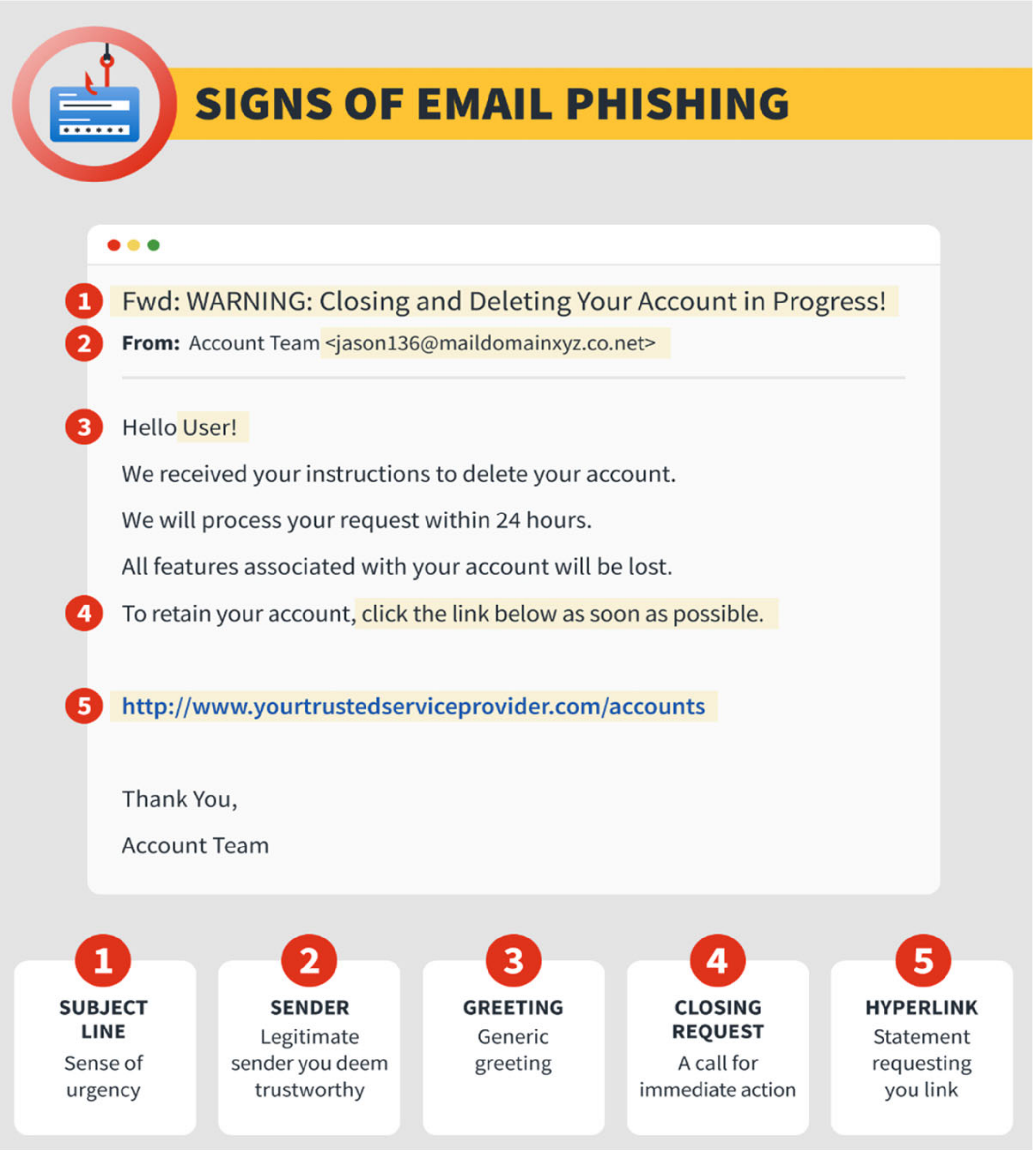
Password Management can be dizzying and emotionally draining just trying to remember work and home passwords! Look at the apps on your devices – can you really remember **ALL** of those passwords?

Pay attention to “friends” or “connections” on social media that get “hacked” and **DO NOT** click on links from Social Media Outlets claiming there are issues with your accounts – this is a hi-jack attempt and you **WILL NOT** recover the account if it gets compromised.

There are some good password managers out there for **PERSONAL** use.

DO NOT install these applications on work devices without IT/Cyber approval first!

Have a good recovery email account for these applications and keep them up to date with security patches!



SIGNS OF EMAIL PHISHING

1 Fwd: WARNING: Closing and Deleting Your Account in Progress!

2 **From:** Account Team <jason136@maildomainxyz.co.net>

3 Hello User!

We received your instructions to delete your account.

We will process your request within 24 hours.

All features associated with your account will be lost.

4 To retain your account, click the link below as soon as possible.

5 http://www.yourtrustedserviceprovider.com/accounts

Thank You,

Account Team

1 **SUBJECT LINE** Sense of urgency

2 **SENDER** Legitimate sender you deem trustworthy

3 **GREETING** Generic greeting

4 **CLOSING REQUEST** A call for immediate action

5 **HYPERLINK** Statement requesting you link

EMAIL PHISHING!

Phishing is the most common cyber attack method experienced by individual and organizations.

In less than **10 MINUTES** an organization can experience devasting effects which range from:

- Loss of sensitive organizational and personal data which could carry reportable penalties at State/Local or Federal Levels
- Impacts to business relationships which become affected by a phishing attack
- Loss of availability (assets, accounts, networks)

Look for these signs when you receive a request to JUST CLICK THE LINK!

Phishing Social Media Accounts

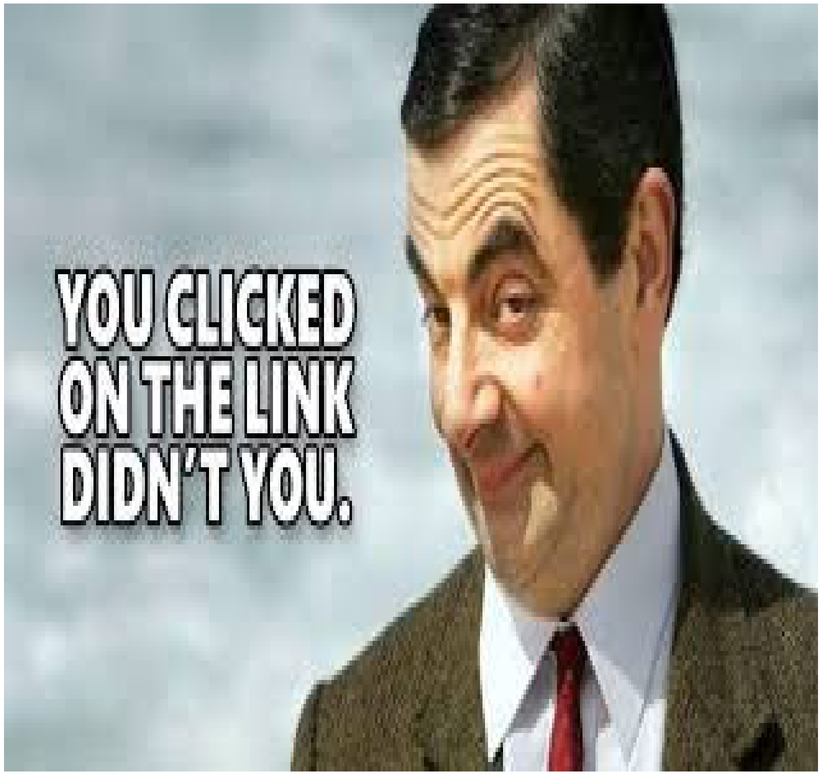
- Phishing Social Media Accounts is when a cyber attacker uses a site like Facebook, Twitter and Instagram in stead of email to hijack sensitive personal information or entices a user to click a malicious link.

- The most common attack is impersonation of people you don't have to be popular to be hacked!

- **PROTECT YOURSELF!**
- Check your **PRIVACY SETTINGS** especially after an update
- Keep Software up to date for the app and your device
- Quizzes: **STOP TAKING THESE**
- Shopping or clicking on links within Facebook
- Create a rescue account and enable **MFA**

You Clicked The Link – Now What!

It happens to the best of us – we are in a rush or we aren't paying attention or we see a familiar name and just click on the link!



Let me run you through what happens after you click a link or even worse enter your password into a suspicious website:

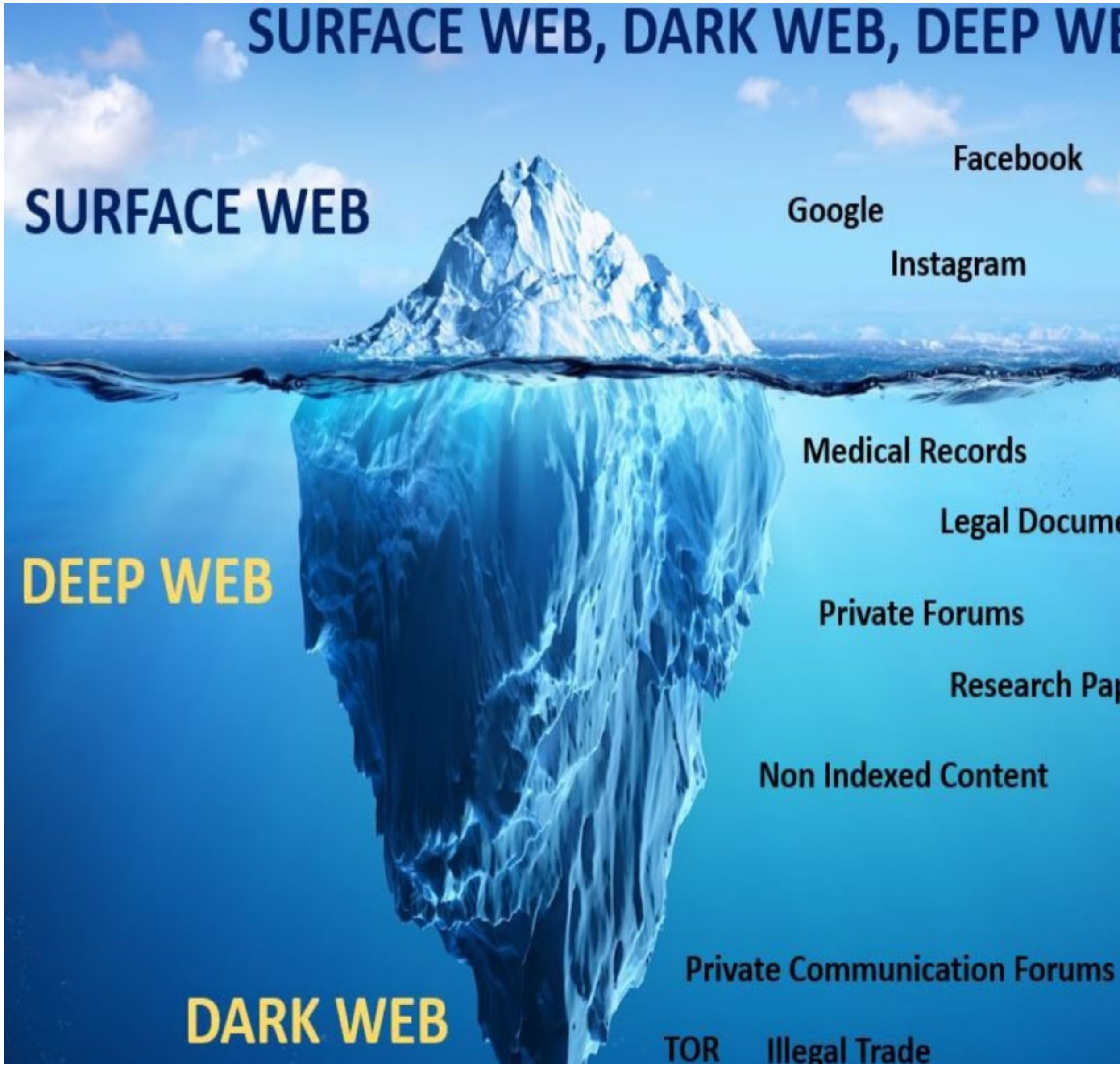
- Once you click the link you are activating a script which spreads like poison across multiple areas within the enterprise
  - Active Directory (AD) - Administrator and Service Accounts are targeted
  - Exchange – Emails begin in seconds to **EVERYONE** in your address book
  - Group Security Policies are targeted for modification
  - Permissions are altered to allow for future backdoor
  - Exfiltration of data begins against shared drives, SharePoint sites and virtual environments
  - Sometimes Ransomware is left behind with a timer

Scripting makes all of these activities possible in seconds!

happens to the best of us – we are in a rush or we aren't paying attention or we see a familiar name and just click on the link!

My Data Went Where?

- The web has quickly become complex and cyber criminals have multiple avenues for selling the data they steal!
- The Deep and Dark Web are layers of the internet that are highly restricted and common users don't just "stumble" onto these websites
- They are masked utilizing anonymized search tools such as TOR which allow a user to hide their digital footprints by relaying their browsing activities across multiple servers located around the world
- Drugs, The Silk Road, Human Trafficking, Murder for Hire, Social Security Numbers, Fake IDs even Human Organs are all for sale in numerous "market places" on the Dark Web
- Pages of compromised logins are for sale for pennies on the dollar!



Apps Collect and Sell Your Data!

- Apps typically need **YOUR** permission to access data from your phone. However, we're human and we don't always read the agreements – you just click "ok" and install!

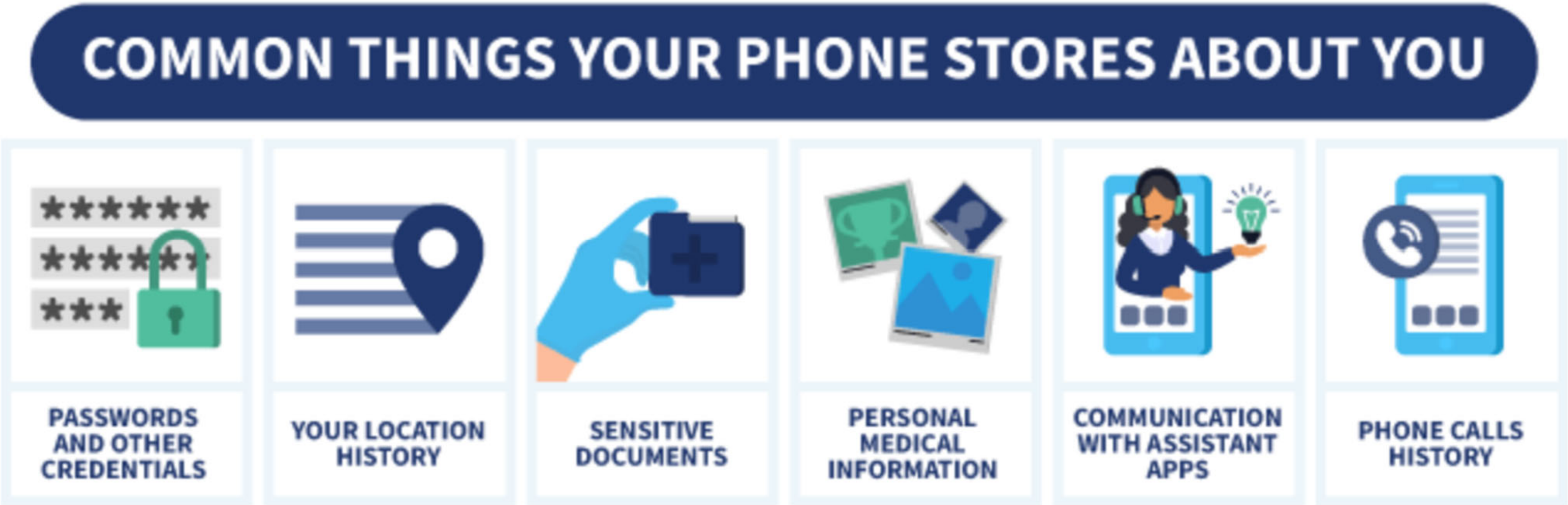
- Even reputable apps like Facebook, Instagram or Twitter collect as much data as they can using your smartphone's settings. Many capture **YOUR** location, browsing history, credentials, and plenty more parameters to understand who you are and what you respond to. They then sell this data to advertisers, so you're more likely to buy whatever they sell via targeted marketing.

- Most people are oblivious to the purpose behind those targeted ads and are willing to give up privacy for relevant ads or a "Free" app.
- **YOUR** data on **YOUR** phone collects about you to be easily available to advertisers, especially since that data can fall into the wrong hands after a breach.

Smart Phone Data Collections

- It’s safe to say that hackers shouldn’t get their hands on **YOUR** data. If you want to improve the security on your smartphone and keep your valuable personal information away from prying eyes I suggest the following:

- **Manage** app permissions. Don’t let apps track everything you do. Try the option of “only while using the app” setting
- **Encrypt** your data on your phone and SD card as well.
- **Delete** old apps. They’re just cluttering your phone but they are collecting data in the background.
- **Lock** your phone with a PIN, passcode, fingerprint, or Face ID. If you use biometrics make sure you remember your passcode/PIN
- **Enable** a Find My Device service in case you lose the device
- Don’t postpone **updates**. They contain valuable safety features against the latest cyber threats.
- **Siri** is a snitch so consider what data she gives away!


COMMON THINGS YOUR PHONE STORES ABOUT YOU
PASSWORDS AND OTHER CREDENTIALS
YOUR LOCATION HISTORY
SENSITIVE DOCUMENTS
PERSONAL MEDICAL INFORMATION
COMMUNICATION WITH ASSISTANT APPS
PHONE CALLS HISTORY

Smart Phone Data Collections

- Smartphones feel like a major body part or critical organ at this point as we develop dependencies on these devices to manage our lives! But do you know how much data is collected on you?

- From where we go, what we like, to who we talk to, and even what credentials we use to log into mobile banking services.

- You might not worry about third-party apps collecting data on you because that app might be saving you time, managing a task or tracking a health aspect of your life but always pay attention to the data these apps collect on you!

Who Else Is Listening?

- Do you ever look at Facebook and wonder why you're seeing a particular ad in your feed?
- Maybe you had been having a conversation with someone and never even conducted a search?
- Apps **spying on you through your phone's microphone** is not make-believe. It's a real, documented phenomenon.
- More and more apps listen for any identifiable shows or movies even conversations in the background. This information is then added to your user profile and used to show you targeted ads.
- Siri works the same way – it's called a Passive Mode where she listens and "offers" assistance if she thinks you need help.
- Add the Hacker to the mix and the potential of them gaining access to you phone would allow them to access your camera or microphone and track everything that feeds through that.
- Your smartphone becomes a listening device allowing an intruder to listen and watch unbeknownst

Security Breechs Are Data Yard Sales!

- How many of us pay attention to the developers or third parties which design apps to respectfully handle **YOUR** data.
- You **can't trust the hacker breaching a third party's database** to handle **YOUR** data responsibly.
- There were over 4,100 security breaches in 2022, exposing over 22 billion records. Apps big and small were impacted
- Apps collect so much data about smartphone users. That data may be safe with Facebook, Google, or Snapchat (it's not, Cambridge Analytica proved that).
- Hackers aren't the only one's paying for data!
- But the moment a data breach happens, **cybercriminals gain access to all that personal information** and begin selling it
- They can steal your passwords, bank details, browsing history, and plenty more.
- They can even gain access to sensitive medical data if they breach a period-tracking app, for example.

Keeping Your Data Secure

1 MANAGE APP PERMISSIONS

2 ENCRYPT YOUR DATA

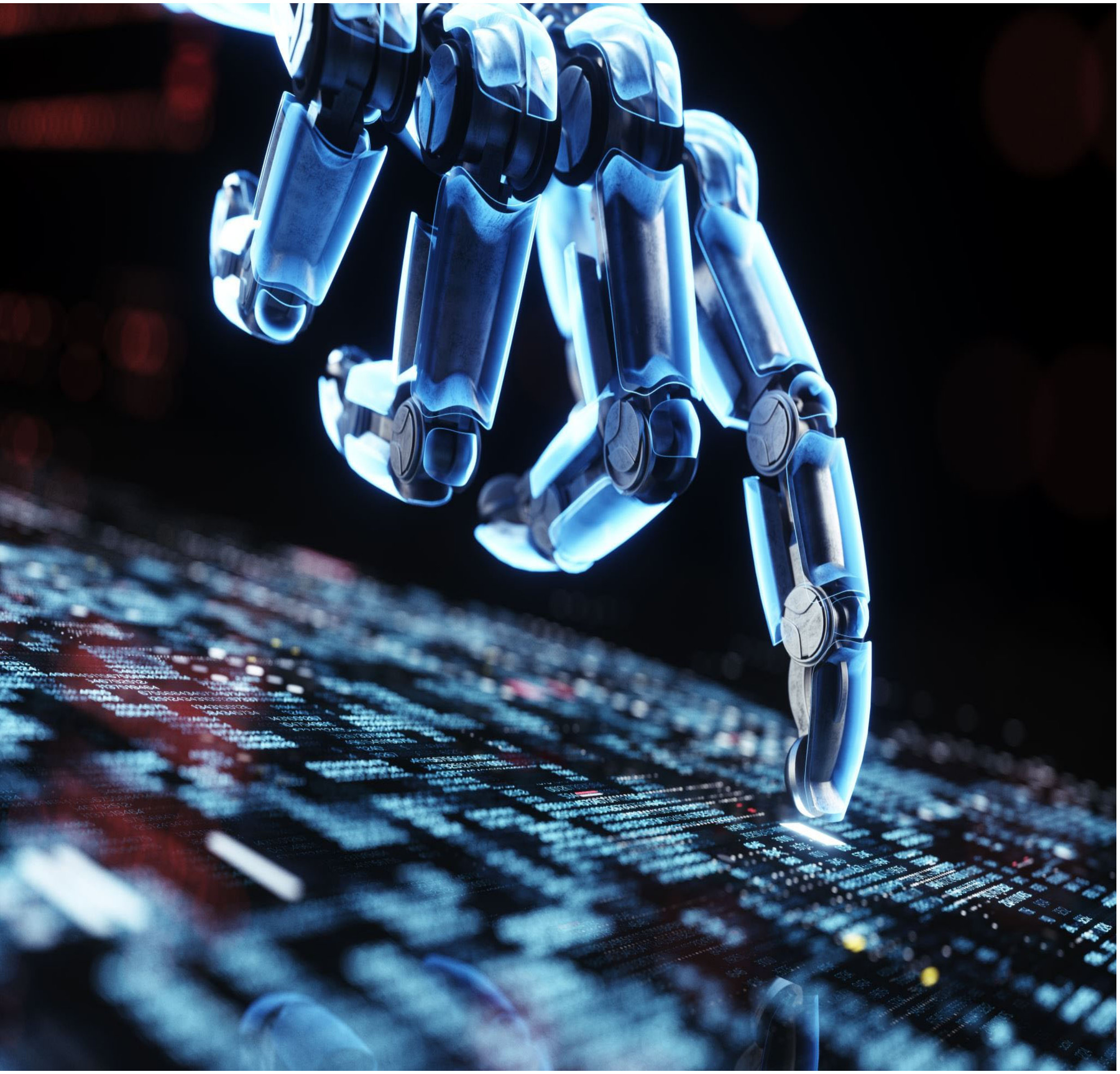
3 DELETE OLD APPS

4 LOCK YOUR PHONE

5 ENABLE FIND MY DEVICE SERVICES

6 DON'T POSTPONE UPDATES

7 INSTALL SECURITY-ENHANCING APPS



Digital Assistants

- Maybe you got one at an office party or as a gift but the following devices have vulnerabilities you should be aware of:

  - Alexa Enabled Devices
  - Siri Enabled Devices
  - Google Smart Devices

- These devices have “machine learning” which enables them to learn your voice, speaking habits, and interests so that they can “assist” you in doing simple tasks.
- Information you ask your Alexa device is not only collected by Amazon and third-party tracking services, but also shared with as many as 40 advertising partners. This data generates ad auction bids from advertisers that are as much as 30x higher than bids without this information.
- Be careful what conversations you have in the presence of these devices.

Home Alarms & Cyber Criminals

Home Alarms protect us and our valuables and it’s important to make sure the basics are done on an annual basis:

- If you have a physical box system (far right image) there is a backup battery (usually a 9V battery) that should be replaced annually. I don’t recommend using a cheap battery from the dollar store!
- If you use a private monitoring service (Brinks, ATS, ect) make sure you have updated your duress words and who has access to the alarm system. If you got a divorce or sold the house update the information immediately.
- For alarm systems that have an “app” make sure you have a strong password or utilize a biometric to gain access. If you get rid of your device delete the app immediately!
- Ring Users make sure you enable STRONG passwords (12-14 characters with upper/lower case letters, special characters symbols and numbers).

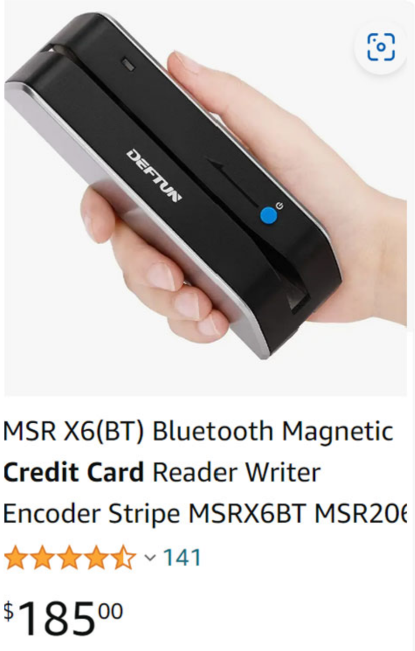
Video Game Systems

Video game systems have greatly evolved since the days of Atari and now allow gamers to connect and play highly realistic games from across the globe!

Cyber Criminals have targeted game systems and gaming networks for the past few years and successfully stolen credit and user information. Here are some tips to secure these accounts:

- For gaming systems to be used by children **UNDER 13** consider enabling the **PARENTAL CONTROLS (SETTINGS)**
- For gaming systems to be used by teens consider adding an adult account to the system in case there is a data compromise or situation that warrants parental involvement
- For gaming systems to be used by adults consider creating a rescue account in case of a compromise of the system or account and write the account information down
- Make sure the passwords used for accounts are **STRONG**
- **NEVER** put your **REAL ADDRESS** for the location
- For kids accounts use a parent’s email address to register the account and never use their **FULL NAMES** for account screen names
- **NEVER** associate a credit card with the accounts – consider getting a disposable gift card to register the account – all three of these systems have gift ards
- Talk to your kids about what information they can share with people they might “game” with and when they should come to you for help.
- **DO NOT** leave cameras enabled on game systems, when you’re done with it disconnect it!
- Research games **BEFORE** you give them to kids – some games have age restrictions for a reason!
- Consider a Wi-Fi channel for the gaming system – some routers will enable you to “split” the signal. This is basically throttling the connection so the gaming system doesn’t eat all the bandwidth.

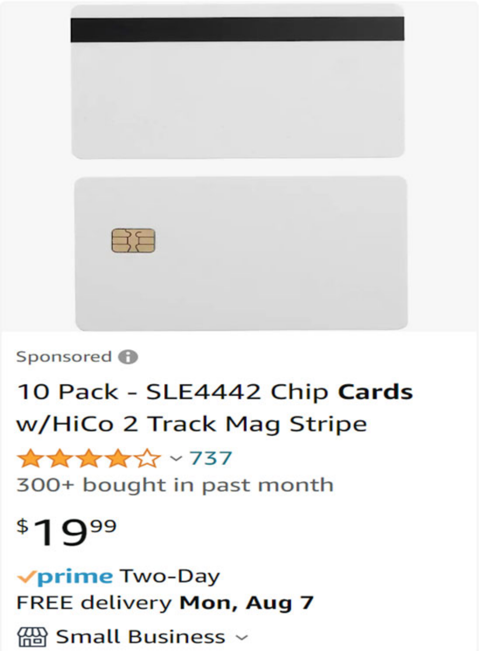
Cyber Criminals Print Their Own Cards!



MSR X6(BT) Bluetooth Magnetic **Credit Card** Reader Writer Encoder Stripe MSRX6BT MSR20

★★★★☆ 141

$\$185^{00}$



Sponsored

10 Pack - SLE4442 Chip **Cards** w/HiCo 2 Track Mag Stripe

★★★★☆ 737

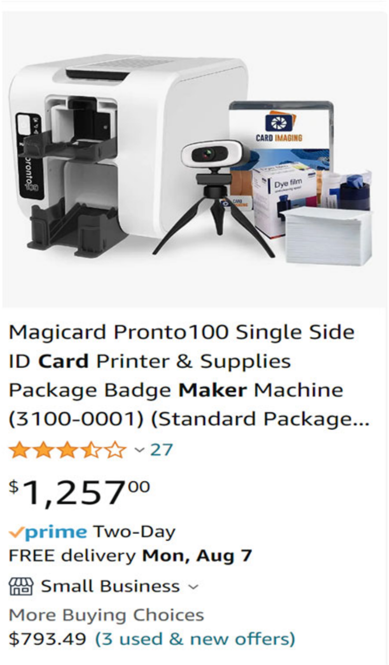
300+ bought in past month

$\$19^{99}$

prime Two-Day

FREE delivery **Mon, Aug 7**

Small Business



Magicard Pronto100 Single Side ID **Card** Printer & Supplies Package Badge **Maker** Machine (3100-0001) (Standard Package...

★★★☆☆ 27

$\$1,257^{00}$

prime Two-Day

FREE delivery **Mon, Aug 7**

Small Business

More Buying Choices

$793.49 (3 used & new offers)

https://youtu.be/vmajlKJIT3U

Gift Card Scams!

Looks for cards that have their validation codes scratched off – don't buy cards that have been scratched!

Save the gift card receipts in case the card doesn't work!

Remember some cards expire and others don't – if you re-gift a gift card make sure it's valid!

Register the cards (Visa, Mastercard, AMEX) if you plan to use them on-line.

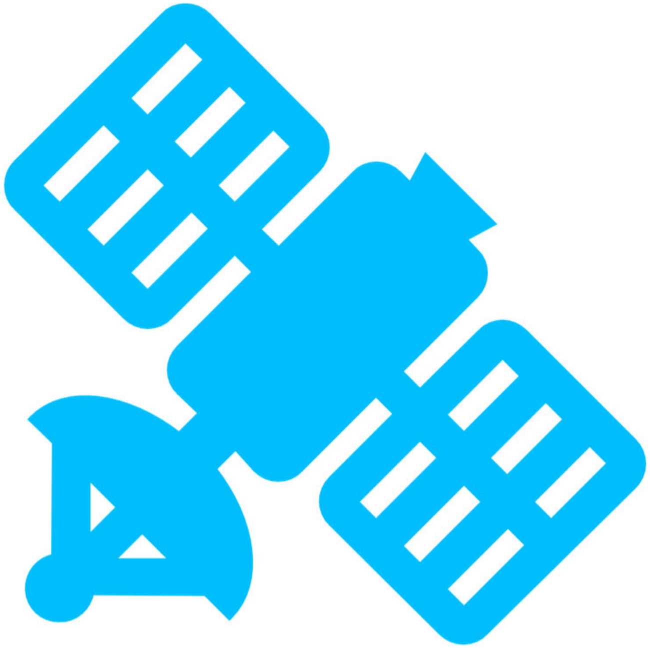
Cards that you don't use or want can be sold to third parties – here are a few recommendations:

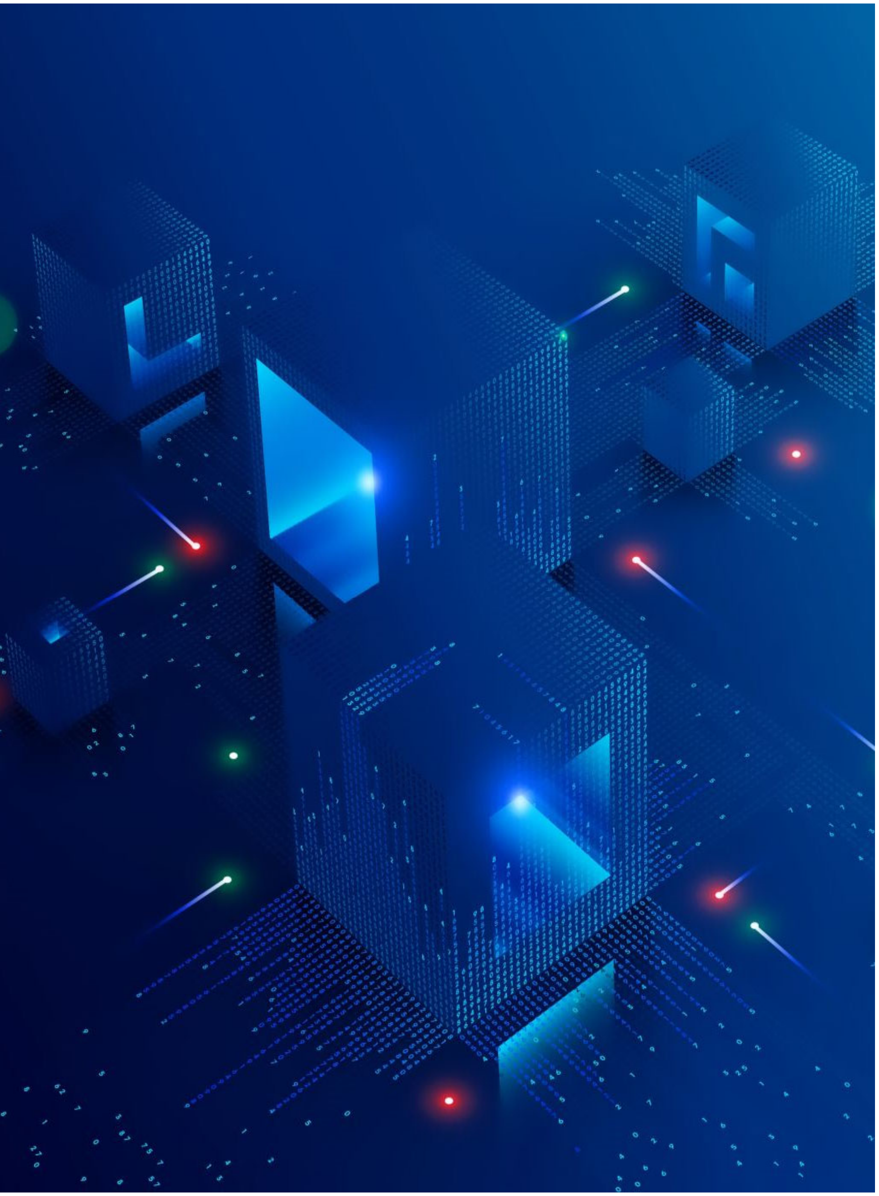
- www.cardcash.com
- www.clipkard.com
- www.giftcash.com

Remember Management WILL NEVER ask you to use a corporate card to buy gift cards on their behalf via a text message – if you get a request CALL the requestor!

GPS – Digital Bread Crumbs

- **YOUR** Location data is mostly tracked through GPS – some apps require it
- Here's interesting GPS facts:
  - Wi-Fi networks are also used to pinpoint your location
  - And while you can shut off your phone's GPS receiver, Wi-Fi location tracking works even if your Wi-Fi is turned off. (E911)
  - Wi-Fi tracking has become highly accurate.
- A lot of apps access location data due to their function. The GPS data can be used to track your on-line behavior and spending habits which is extremely valuable to advertisers.
- This is why apps can try to collect as much information on you as they can.
- For example, the Facebook tracks your location for "check-in's" and meta tagging of pictures.
- Mapping apps obviously track your trips but did you know that archive resides on your phone and the app feeds data back to third parties without your knowledge





How To Avoid Being a Victim of Credit Card Fraud and ID Theft

- Fraud is becoming more and more prevalent and there are steps you can take to help protect yourself and reduce your risk of falling victim to credit card fraud:

- Only use your card for purchases on websites you **TRUST**.
- **NEVER** enter your card information (or Social Security number, etc.) in response to an email or via an emailed link. **ALWAYS** go directly to the company's site instead of typing the address yourself.
- Use a credit card (**NOT A DEBIT CARD**) to limit your liability for any fraud that may occur.
- Do not give out your card number over the phone unless you initiated the transaction, and you **KNOW** the company is reputable.
- Can you prevent your data from being lost? **NO** you can't control where your data goes or how it's handled once you enter it not a website, online account or provide it to a financial institution.
- Being **AWARE** of what data is lost is critical in preventing being re-victimized. Follow up with the organization that lost your data and know your legal rights for restitution and free credit monitoring.
- Don't be afraid to **CLOSE** a compromised account, even a bank account and re-open the account with a different account number.
- **LIMIT** the amount of personal information you provide to Social Media accounts and monitor these organizations for data breaches – it's your data!
- Credit Monitoring tools are becoming more and more important in your Data Self Defense Kit!
- Your **KIDS** data needs to be monitored because they can be victims years before you realize it!

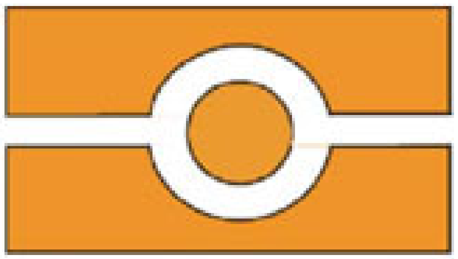
Reporting

- When you find out you’ve been a victim of identity theft or on-line fraud there are steps that are recommended to stop the problem from escalating:
  - If you have been a victim of an Internet scam, contact the Federal Trade Commission (FTC) at 1-877-FTC-HELP (1-877-382-4357) or use their online features to file a report.
    - ReportFraud.ftc.gov
    - Five tips for reporting a scam | USAGov
  - You can also report to your local police, the FBI, or the FBI's Internet Crime Complaint Center.
    - Report Fraud (justice.gov)
    - https://www.cisa.gov/be-cyber-smart/report-incident
    - Social Security: Fraud Prevention and Reporting | SSA

Cyber Criminals Target More Than Bank Accounts!

- U.S. Passports:
- RFID microchips have been embedded inside all passports issued since 2007 and securely store personal contact information. These chips are inside your passport in case it gets lost or stolen
- In order for a passport's RFID chip to be read, it needs to be within six inches of an RF reader. Thanks to a special piece of security tape buried in the cover of your passport, the data on the chip cannot be read when the passport book is closed.
- If scammers steal your passport number, they can impersonate you, create fake travel documents, or even open bank accounts in your name. Unfortunately, even if your physical passport is safely stored away, you could still be at risk.

The below is the universal RFID e-passport logo which is being used to identify passport locations which require e-passport scanning.



As of 2008, 45 countries are using e-passports, and more are expected to follow suit.